



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/419,828	10/14/1999	DON VAN DYKE	M-7084-US	1859
23418	7590	02/08/2005	EXAMINER	
VEDDER PRICE KAUFMAN & KAMMHOLZ 222 N. LASALLE STREET CHICAGO, IL 60601			SMITHERS, MATTHEW	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 02/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/419,828

Applicant(s)

DYKE ET AL.

Examiner

Matthew B Smithers

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on an amendment filed 31 August 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-13 and 15-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-13,15-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION***Response to Arguments***

Applicant's arguments filed 31 August 2004 have been fully considered but they are not persuasive.

Applicant argues Jones does not disclose a register file providing operands to an ALU. Examiner contends Figure 3 clearly show a register file (element 58) sends data to an ALU (element 56). In the disclosure section that corresponds with Figure 3 (column 7, lines 15-19), Jones discloses an embodiment where the ALU operates on a 32-bit word received from the register file. The disclosure goes further in discussing how any register can be used as an operand to any instruction (see column 7, line 65 to column 8, line 29). This section makes it clear that any register can be used to enhance the instruction set performing the necessary operations within the cryptographic procedure. In the same section (see column 7, lines 15-19), Jones teaches the register file is made up of 8-16 32-bit registers. These registers provide the ALU with its stored contents in conjunction with an instruction from a processing element memory. As applicant points out in his remarks of August 31, 2004, general purpose registers are addressable for different purposes. One of the purposes is to temporarily store calculated data in an accumulator until the data is needed in a subsequent calculation. This is shown in an example using the DES algorithm (see column 16, line 57 to column 18, line 13). Based on the above arguments, the examiner maintains the previous rejection.

Claim Rejections - 35 USC § 102

Art Unit: 2137

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 3-13, and 15-21 are rejected under 35 U.S.C. 102(e) as being anticipated by U. S. patent 6,088,800 granted to Jones et al.

Regarding claim 1, Jones meets the claimed limitations as follows:

"A computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations

wherein said computer system further comprises a register file providing operands to said arithmetic logic unit; and

wherein said register file includes general purpose registers." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 3, Jones meets the claimed limitations as follows:

"The method of claim 1, wherein said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey." see column 6,

Art Unit: 2137

lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 4, Jones meets the claimed limitations as follows:

"The computer system of Claim 3, wherein said datum is 64 bits long and said subkey is 48 bits long." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14. See sample code in column 17, where A (first datum is loaded in register 1); B (second datum loaded in register 2) and K (subkeys computed and stored in advance in order to XOR with the expanded group)(see column 17, lines 1-14).

Regarding claim 5, Jones meets the claimed limitations as follows:

"The computer system of Claim 3, wherein said first and second portions each contain one-half number of bits of said datum." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 6, Jones meets the claimed limitations as follows:

"The computer system of Claim 5, wherein each of said first and second portions is 32 bits long." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 7, Jones meets the claimed limitations as follows:

"The computer system of Claim 3, wherein said first, second and third registers store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in

Art Unit: 2137

said first, second and third registers to be operands in a subsequent execution of said instruction." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 8, Jones meets the claimed limitations as follows:

"The computer system, of Claim 7, wherein a bypass mechanism is provided in said register file such that said results are provided as input to said logic circuit without first being written back to said first, second and third registers." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 9, Jones meets the claimed limitations as follows:

"The computer system of Claim 8, wherein said register file and said bypass mechanism are shared by all instructions in said arithmetic logic unit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 10, Jones meets the claimed limitations as follows:

"The computer system of Claim 1, further comprising a second logic circuit capable of performing key selection for said DES algorithm, said second logic circuit operating in parallel with said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 11, Jones meets the claimed limitations as follows:

Art Unit: 2137

"The computer system of Claim 1, wherein said logic circuit further comprises a circuit for selecting a subkey from a key." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 12, Jones meets the claimed limitations as follows:

"The computer system of Claim 11, wherein said key is 56 bits long." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 13, Jones meets the claimed limitations as follows:

"A process for performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising: providing a logic circuit in an arithmetic logic unit; and performing expansion permutation, S-box substitution and P-box permutation and associated XOR operations in said logic circuit; and storing operands in a register file; and providing said operands to said logic circuit; wherein said register file includes general purpose registers." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 15, Jones meets the claimed limitations as follows:

"The process of Claim 13, further comprising: storing operands in a register file; and providing said operands to said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 16, Jones meets the claimed limitations as follows:

"The process of Claim 15, further comprising: storing a first portion of a datum for said encryption or decryption in first register in said register file; storing a second portion of

Art Unit: 2137

said datum for said encryption or decryption in second register in said register file; and storing a subkey for said encryption or decryption in third register in said register file." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 17, Jones meets the claimed limitations as follows:

"The process of Claim 16, further comprising storing operands of an instruction executing one round of said DES algorithm in said first, second and third registers using said logic circuit and said shift circuit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 18, Jones meets the claimed limitations as follows:

"The process of Claim 17, further comprising providing said results as input to said logic circuit without first being written back to said first, second and third registers." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 19, Jones meets the claimed limitations as follows:

"The process of Claim 13, further comprising selecting a subkey from a key for said DES algorithm in a second logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 20, Jones meets the claimed limitations as follows:

Art Unit: 2137

"The process of Claim 19, further comprising operating said second logic circuit in parallel with said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 21, Jones meets the claimed limitations as follows:

"The process of Claim 13, further comprising selecting a subkey from a key using a key select circuit in said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 22, Jones meets the claimed limitations as follows:

"A computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising: an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations;

wherein said computer system further comprises a register file providing operands to said arithmetic logic unit; and

wherein said register file includes general purpose registers to store at least two of attributes parameters datapath, control, L_i's, R_i's, and subkeys K_i's." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 23, Jones meets the claimed limitations as follows:

"The method of claim 1, wherein said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey." see column 6,

Art Unit: 2137

lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14. See sample code in column 17, where A (first datum is loaded in register 1); B (second datum loaded in register 2) and K (subkeys computed and stored in advance in order to XOR with the expanded group)(see column 17, lines 1-14).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

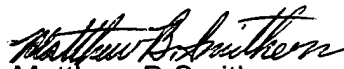
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew T Caldwell can be reached on (571) 272-3868. The fax phone

Art Unit: 2137

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew B Smithers
Primary Examiner
Art Unit 2137